

SUPERIOR COURT OF WASHINGTON
COUNTY OF KING

VIX TECHNOLOGY USA, Inc.,

Plaintiff,

v.

CENTRAL PUGET SOUND REGIONAL
TRANSIT AUTHORITY (dba SOUND
TRANSIT) and KEVIN WALLACE,

Defendants.

No. 18-2-19467-9

RESPONSE IN OPPOSITION TO
MOTION FOR TEMPORARY
RESTRAINING ORDER AND
PRELIMINARY INJUNCTION

I. INTRODUCTION AND RELIEF REQUESTED

Vix Technology must prove that the Sound Transit records at issue are both exempt from disclosure and clearly not of public interest. It has not done so. In fact, the requested software applications encompass fare enforcement procedures which are supposed to prevent discrimination, and which vest machines with the “use of discretion” that once was exercised by enforcement officers. The public has an interest in knowing how Sound Transit enforces fare requirements on buses and trains, and cannot learn the whole story without the applications used on fare devices. Because Vix Technology has not and cannot meet the injunction standard under the Public Records Act, RCW 42.56.540, the motion should be denied.

1 II. EVIDENCE RELIED UPON

2 This response relies upon the record of the case and the declarations of Kevin Wallace and
3 Katherine George, and attachments thereto.

4 III. STATEMENT OF FACTS

5 Kevin Wallace is a transit user. Declaration of Kevin Wallace, ¶2. On January 13, 2018, he
6 made a public records request to Sound Transit for all “guidebooks, policy manuals and similar
7 materials regularly provided to persons designated as fare enforcement monitors by Sound Transit
8 under RCW 81.112.210.” Wallace Dec., ¶3, Ex. A, p. 1. In response, Sound Transit produced 13
9 “standard operating procedures” for fare enforcement officers. Wallace Dec., ¶4. These documents
10 outlined procedures for basic on-board train inspections, proof of payment inspection techniques,
11 writing and issuing warnings and citations, filing a third-degree theft case, handling juveniles,
12 confiscating university and college passes, fare inspection rules, and non-discrimination. *Id.*

13 One of the produced documents, SOP-SEC 10-21, explains “the basics of inspections where
14 proof of payment is presented in the form of an ORCA card.” Wallace Dec., ¶5 and Ex. B, p. 1. It
15 defines an ORCA card as “a plastic card that has an electronic chip that is used for fare payment.”
16 *Id.* The document says: “If the ORCA card has an E-purse and is not tapped or has no value loaded
17 on it, this constitutes a violation of the Proof of Payment section of RCW 81.112.220,” punishable
18 by a \$124 fine. Ex. B, pp. 1-2. It directs the enforcement officer to scan the passenger’s ORCA
19 Card with a “handheld ORCA App to determine if the card was tapped prior to boarding.” Ex. B, p.
20 2. According to SOP-SEC 10.21, the ORCA Inspection App is used on Link light rail and Sounder
21 commuter trains to check ORCA cards for payment. Ex. B, p. 3. The document cautions: “Not all
22 passengers understand the ORCA system,” and directs officers to explain how it works rather than
23 simply say, “You did not tap.” *Id.*

1 Another document produced by Sound Transit, SOP-SEC 10-20, “outlines how Fare
2 Inspections are monitored to assure discrimination does not occur.” Wallace Dec., ¶6, Ex. C, p. 1.
3 It states, “Use of discretion is further outlined in SOP-SEC 10-07.” *Id.* However, Sound Transit
4 did not produce SOP-SEC 10-07 in response to Mr. Wallace’s request for fare enforcement policies
5 and guidebooks. Wallace Dec., ¶¶7-8 and Ex. A., pp. 3 and 6. When asked about the missing
6 document, Sound Transit Project Coordinator Leigh Tennison said in an April 25, 2018 email:

7 We have met with security staff and 10-7 is no longer included in the SOPs. *It refers*
8 *to a process used when fare enforcement officers manually issued tickets. This*
9 *process is now done automatically through the hand held devices* and therefore 10-7
10 is no longer included.

11 Wallace Dec., Ex. A, p. 6 (italics added).

12 Mr. Wallace was concerned that officer discretion had been replaced with machines acting
13 “automatically.” Wallace Dec., ¶9. This was especially alarming because, according to the
14 procedures, people can be charged with theft based on information on the hand-held machines. *Id.*

15 In order to learn how the hand-held devices “automatically” exercised the discretion that
16 was previously vested in fare enforcement officers, Mr. Wallace made another records request on
17 May 5, 2018 for the software applications referenced in the enforcement procedures. Wallace Dec.,
18 ¶10 and Ex. D, p. 1. Specifically, he asked for:

19 A copy of the latest version of each of the following applications used on Fare
20 Enforcement handheld devices:

- 21 - Orca Inspection
- 22 - Officer Android

23 *Id.* On May 11, 2018, he received the following response from Ms. Tennison:

24 DRAFT-for your approval. This is due today or Monday at the latest. We don't have
an "officer android" app. The ORCA Inspection is an android app.

This will acknowledge your request for a copy of the latest version of each of the
following applications used on fare enforcement handheld devices:
-ORCA Inspection

1 -Officer Android

2 We received your request on May 7, 2018.

3 The application used to scan ORCA cards is called "ORCA Inspection." It is an
4 Android version. We are unable to provide you with this app because it is exempt
5 under RCW 42.56.270(1). This completes our response and we will close this
6 request file.

7 Ex. D, pp. 1-2. Although the first word was "DRAFT," Mr. Wallace understood the response to be
8 official. Wallace Dec., ¶11. The citation to an exemption, and the closing of the request, indicated
9 that Sound Transit had done legal research and formed a position against disclosure. *Id.*

10 Later that day, Mr. Wallace replied in pertinent part as follows:

11 I appeal. RCW 42.56.270(1) only exempts disclosure of software when such
12 disclosure "would produce private gain and public loss" which is not the case here --
13 the released records are being made available to the public. They are being requested
14 in the interest of increased transparency around the fare enforcement process, not for
15 private gain of any kind. On 4/25, in response to request PD18-030, you indicated to
16 me that fare enforcement policy SOP-SEC 10-07 has been superseded by a process
17 in the application that I am now requesting. Fare enforcement policy is a matter of
18 public record, even when it's embodied in software.

19 Ex. D, pp. 2-3.

20 On May 14, 2018, Sound Transit paralegal Q'Deene Nagasawa told Mr. Wallace that Ms.
21 Tennison's email was sent inadvertently and that her own "initial review" suggested that RCW
22 42.56.270(1) did not apply. Wallace Dec., ¶12 and Ex. D, p. 3. However, she stated she needed
23 more time "to review." *Id.* Final results of that review were never communicated to Mr. Wallace.
24 Wallace Dec., ¶15. Instead, Sound Transit put the request on hold while waiting for Vix
Technology to bring this action. Wallace Dec., ¶¶13-14. Then, on August 13, 2018 – three months
after sending inconclusive messages about exemption claims - Sound Transit told Mr. Wallace that
it would not take action on his request due to this lawsuit. Wallace Dec., ¶14 and Ex. D, p. 8.

Mr. Wallace testified:

1 I believe the general public, like me, has an interest in the requested records. If
2 humans were still carrying out Sound Transit's 'use of discretion' procedures,
3 nobody would question that they should be public. Software, in general, is a way of
4 codifying procedures. The ORCA Inspection and Officer Android software
5 applications are carrying out procedures that used to be performed by humans. I
6 believe it is important for the public to know whether these applications are actually
7 preventing discrimination in fare enforcement. More generally, taxpayers and transit
8 riders like me are interested in how enforcement by machines works.

9 I'm a software engineer myself. I disagree that releasing software, by itself, makes it
10 insecure. If the software is competently written and if security keys are redacted,
11 confidential financial information would be protected.

12 Wallace Dec., ¶¶16-17.

13 Vix Technology, formerly called ERG Transit Systems, has a \$39 million contract with
14 Sound Transit and six other transit agencies to develop, operate and maintain a regional fare
15 coordination system. Declaration of Katherine George, Ex. A, p. 1. Of that amount, Sound
16 Transit's share is \$6.8 million. *Id.* There was no competition for the contract. George Dec., Ex. B,
17 p. 1. Sound Transit received two proposals, but determined that "only one firm" – Vix Technology
18 – met requirements of the contract proposal. *Id.*

19 IV. STATEMENT OF ISSUE

20 The issue is whether to enjoin disclosure of software applications pursuant to RCW
21 42.56.540 when the applications are public records containing fare enforcement procedures of
22 interest to the public, when the plaintiff appears to have no competitors capable of exploiting the
23 information, and when no specific exemption applies.

24 V. AUTHORITY

"Under the Public Records Act (PRA), public records may be withheld only 'in accordance
with a statute that exempts or prohibits disclosure in whole or in part of specific information or
records.' " *Lyft Inc. v. City of Seattle*, 190 Wn.2d 769, 777 (2018), quoting *Progressive Animal
Welfare Society v. Univ. of Wash.*, 125 Wn.2d 243, 251-52 (1994) ("PAWS"). The PRA "begins

1 with a mandate of full disclosure of public records; that mandate is then limited only by the precise,
2 specific, and limited exemptions which the Act provides.” *Lyft* at 778, quoting *PAWS*, 125 Wn.2d at
3 258. See also RCW 42.56.070(1) (requiring each agency to make available all public records
4 unless they fall within specific exemptions of the PRA “or other statute which exempts or prohibits
5 disclosure of specific information or records”). Here, it is not disputed that the software
6 applications at issue are public records as defined by RCW 42.56.010.

7 Vix Technology brought this “reverse” PRA action under RCW 42.56.540, which states:

8 The examination of any specific public record may be enjoined if, upon motion and
9 affidavit by...a person who is named in the record or to whom the record specifically
10 pertains, the superior court...finds that such examination would clearly not be in the
public interest and would substantially and irreparably damage any person, or would
substantially and irreparably damage vital governmental functions.

11 To obtain an injunction, Vix Technology must show “that a specific exemption applies *and* that
12 disclosure would not be in the public interest and would substantially and irreparably damage a
13 person or a vital government interest.” *Lyft*, 190 Wn.2d at 786, citing *Soter v. Cowles Publishing*
14 *Co.*, 162 Wn.2d 716, 757 (2007) and *Morgan v. City of Federal Way*, 166 Wn.2d 747, 756-77
15 (2009). Thus, even if this Court found that an exemption applies (which is not the case), it would
16 not be enough. *Lyft* at 786. Neither the exemption test nor the public interest test is met here.

17 A. The Software Applications Are Not Exempt.

18 Vix Technology asserts three exemptions from disclosure. RCW 42.56.270(11) is the most
19 easily dispensed. Vix Technology contends that the applications are “trade secrets” protected under
20 RCW 42.56.270(11). But that statute, on its face, applies only to health care records. It protects:

21 Proprietary data, trade secrets, or other information that relates to: (a) A vendor's
22 unique methods of conducting business; (b) data unique to the product or services of
23 the vendor; or (c) determining prices or rates to be charged for services, *submitted by*
24 *any vendor to the department of social and health services or the health care*
authority for purposes of the development, acquisition, or implementation of state
purchased health care as defined in RCW 41.05.011.

1 RCW 42.56.270(11) (*italics added.*) The software applications were submitted to Sound Transit,
2 not the Department of Social and Health Services or the Health Care Authority, and therefore are
3 not subject to the exemption. *Id.*

4 To argue otherwise is to make half of the statute superfluous, contrary to principles of
5 statutory construction. Courts give effect to all the language in a statute and harmonize all its
6 provisions. *Ockerman v. King County Dep't of Dev. & Env't'l Servs.*, 102 Wn. App. 212, 216
7 (2000). The plaintiff's interpretation would strip the phrase "submitted by any vendor to the
8 department of social and health services or the health care authority for purposes of the
9 development, acquisition, or implementation of state purchased health care as defined in RCW
10 41.05.011" of any effect. RCW 42.56.270(11). It also would violate RCW 42.56.030, which
11 requires narrow construction of PRA exemptions to promote full disclosure "and to assure that the
12 public interest will be fully protected." RCW 42.56.030. *See also Bonamy v. City of Seattle*, 92
13 Wn. App. 403, 408-409 (1998) (courts should view with caution any interpretation which frustrates
14 the PRA purpose of disclosure).

15 Vix Technology is interpreting RCW 42.56.270(11) as a general exemption for trade secrets
16 held by any agency. This is wrong. The Washington Supreme Court recently affirmed that no
17 provision of the PRA exempts trade secrets from disclosure. *Lyft*, 190 Wn.2d at 780. Rather, trade
18 secrets are addressed in the Uniform Trade Secrets Act (UTSA), which "was enacted to subsume
19 claims of civil liability for misappropriation of trade secrets." *Id.*, citing RCW 19.108.900(1). The
20 Supreme Court said: "The UTSA contains no specific exemption of trade secrets from public
21 disclosure laws." *Lyft* at 780. The Court further explained that "misappropriation" necessarily
22 involves a record acquired under "a duty to maintain its secrecy," and that a public agency cannot
23 owe such a legal duty. *Lyft* at 787, citing RCW 19.108.010(2)(b)(ii), WAC 44-14-06002(1) ("Any
24

1 agency contract regarding the disclosure of records should recite that the [PRA] controls”), and
2 *Spokane Police Guild v. Liquor Control Bd.*, 112 Wn.2d 30, 40 (1989) (“[P]romises cannot override
3 the requirements of the disclosure law”). In sum, RCW 42.56.270(11) is not an exemption for trade
4 secrets submitted to Sound Transit, and no such exemption exists.

5 B. RCW 42.56.270(1) Also Does Not Apply.

6 Vix Technology also invokes RCW 42.56.270(1), which protects the following “financial,
7 commercial, and proprietary information”:

8 Valuable formulae, designs, drawings, computer source code or object code, and
9 research data obtained by any agency within five years of the request for disclosure
10 *when disclosure would produce private gain and public loss.*

11 (italics added). Vix Technology’s entire argument is that the requested applications constitute
12 “computer source code or object code” received by Sound Transit within the past five years, and
13 that a private party may invoke the exemption. Motion, pp. 9-10. There was no argument that
14 “disclosure would produce private gain and public loss.” *Id.* Nor were the records submitted in
15 camera to establish the extent to which sensitive “source code or object code” is implicated, and
16 whether redactions of sensitive details are possible. RCW 42.56.210(1) (exemptions are
17 inapplicable to the extent that information threatening privacy interests can be deleted). The
18 plaintiff’s cursory treatment of this exemption falls far short of proving it applies here.

19 Vix Technology argued, in support of a different exemption claim, that “public loss” would
20 result from disclosing the ORCA Inspection App because it allows transit operators to adjust values
21 on ORCA Cards through interaction with “confidential customer (rider) information.” Motion, pp.
22 8-9. The fear is that hackers could “reverse engineer how to fraudulently add and subtract money
23 or fare products to individual ORCA fare cards.” Motion, p. 12. But this ignores that Sound
24 Transit can redact security keys to guard against such risks. Moreover, only one of the two

1 applications purportedly could expose confidential rider information. Vix Technology did not
2 establish any risk of public loss from disclosure of Officer Android.

3 As for private gain, Vix Technology makes the bare assertion that disclosure “would
4 substantially injure Vix’s competitive position by eroding its trade secrets, and allowing its
5 competitors to understand exactly how Vix delivers the services it does.” Motion, p. 11. But there
6 is no evidence that Vix has any competitors, let alone that such competitors are maneuvering to
7 “reverse engineer” agency-leased software so as to steal purported secrets. In fact, Sound Transit
8 proclaimed that only one other company sought Vix’s contract, and was not qualified.¹ In sum, Vix
9 has not proven that disclosure of the applications would cause private gain and public loss,
10 particularly with respect to Officer Android. Therefore, RCW 42.56.270(1) does not apply.

11 C. RCW 42.56.420(4) Also Does Not Apply.

12 Finally, Vix Technology invokes the security exemption, RCW 42.56.420(4), without
13 quoting the full statute and without identifying any *specific* information fitting within its narrow
14 scope. Motion, pp. 8-9. The statute protects:

15 Information regarding the public and private infrastructure and security of computer
16 and telecommunications networks, *consisting of security passwords, security access*
17 *codes and programs, access codes for secure software applications, security and*
18 *service recovery plans, security risk assessments, and security test results to the*
extent that they identify specific system vulnerabilities, and other such information
the release of which may increase risk to the confidentiality, integrity, or availability
of security, information technology infrastructure, or assets.

19 RCW 42.56.420(4) (italics added). Vix does not assert that the applications themselves contain the
20 specific types of information covered, i.e., security passwords, security access codes, access codes
21 for security software applications, security and service recovery plans, security risks assessments, or
22 security test results that “identify specific system vulnerabilities.” *Id.*; Motion, p. 8. Rather, Vix

24 ¹ This may explain why Vix reportedly has similar contracts “across the world.” Motion, p. 3.

1 argues that one of the applications, ORCA Inspection, interacts with *other* computer systems that
2 contain “system security protocols.” Motion, p. 8. This vague and extenuated connection simply
3 does not fall within the exemption. Mr. Wallace is not requesting the “system security protocols”
4 in the “back-office computer systems” that transit operators interact with when adjusting ORCA
5 card values. Rather, he requests only the applications themselves, and expects that – as products of
6 a \$39 million contract - they are written competently enough to be secure.

7 Moreover, the motion fails to identify any specific security information associated with
8 Officer Android. With respect to the ORCA Inspection App, Vix again overlooks the possibility of
9 redaction. There is no evidence of any attempt by Sound Transit or Vix Technology to delete
10 whatever unidentified information might provide access to “back-office computer systems.” Mr.
11 Wallace is not interested in security keys. Under RCW 42.56.210(1), the exemption does not apply
12 if the information warranting protection can be redacted. In sum, the vague arguments about one
13 application’s “interaction” with computers, without addressing redaction of whatever access codes
14 or security keys might permit access to security information, fall far short of establishing that the
15 security exemption applies.

16 D. The Public Has An Interest in the Requested Records.

17 Even if Vix Technology had established that an exemption applies, which it did not, the
18 motion still should be denied because of the compelling public interest in Sound Transit’s fare
19 enforcement procedures. The applications are used to check ORCA cards for payment, which can
20 lead to civil fines and theft charges. Thus, their fairness and effectiveness is important to the
21 dignity and liberty of transit riders, while also affecting the financial soundness of the public bus
22 and train system.

1 Importantly, Mr. Wallace's prior records request revealed that the applications contain fare
2 enforcement procedures; that is, they replaced the "use of discretion" procedure which previously
3 was carried out by humans. The former procedure was supposed to prevent discrimination in fare
4 enforcement. Without access to the applications, the public cannot ascertain whether machines are
5 preventing discrimination as effectively as humans did. This is a matter of public interest
6 precluding an injunction under RCW 42.56.540.

7 VI. CONCLUSION

8 For the foregoing reasons, the motion should be denied.

9
10 I certify that this memorandum contains 3,145 words, in compliance with the Local Civil Rules.

11
12 
13 Katherine A. George, WSBA 36288
14 Johnston George LLP
15 126 34th Ave., Suite 307
16 Seattle, Wash. 98122
17 Phone 206 832-1820
18 Fax 206 770-6393
19 kathy@johnstongeorge.com

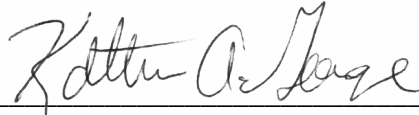
18 CERTIFICATE OF SERVICE

19 I certify that on August 31, 2018, I served the foregoing memorandum and related declarations,
20 with exhibits, to registered parties via the e-service feature within the Clerk's online eFiling
21 application, and by email to:

22 Mark Rosencrantz
23 Carney Badley Spellman, P.S.
24 701 Fifth Avenue, Suite 3600
Seattle WA 98104
rose@carneylaw.com

1 James Niemer
2 Sound Transit
3 401 S. Jackson St.
4 Seattle, WA. 98104

5 james.niemer@soundtransit.org

6 

7 Katherine A. George